Judge Robert J. Bryan

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	NO. CR15-535RJB UNITED STATES' RESPONSE TO DEFENDANT'S MOTION TO COMPEL (FILED UNDER SEAL)

The United States of America, by and through Annette L. Hayes, United States Attorney for the Western District of Washington, S. Kate Vaughan, Assistant United States Attorney for said District, and Keith A. Becker, Trial Attorney, hereby files this response to Defendant's Motion to Compel.

The defendant, Jay Michaud, is charged in this case with receipt and possession of child pornography. The charges arise from an investigation into a website ("Website A") through which registered users like Michaud regularly accessed illegal child pornography. That website operated on the Tor network, which allows its users to mask their Internet Protocol ("IP") addresses, which ordinarily can be used to identify a user, by bouncing user communications around a network of computers before reaching its destination. Michaud's IP address was discovered through the court-authorized use of a

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

Network Investigative Technique ("NIT") that was deployed on the website while it briefly operated under government control.[1]

Michaud seeks disclosure of three categories of items – (1) a copy of the programming code for the court-authorized NIT; (2) the number of site visits and images and videos downloaded or distributed by persons other than him while the website briefly operated under government control; and (3) internal government memoranda related to the approval or supervision of the operation. It is the defendant's burden to show that the requested information is material to his defense. His requests, however, amount to nothing more than a fishing expedition for information that is either not material to his defense or has already been provided. Moreover, in the event the Court were to find that disclosure of the NIT programming code were material to Michaud's defense, that information is protected by a qualified law enforcement privilege. Accordingly, this Court should deny his motion.

I. DISCOVERY REQUESTS AND THE GOVERNMENT'S RESPONSES

On September 9, 2015, the defendant made a discovery request seeking, among other things that he does not seek to compel, information regarding the court-authorized NIT that identified his IP address while he accessed child pornography on "Website A." Ex. 1. In it, the defendant requested "[a] detailed description of the 'additional computer instructions' that are downloaded onto target computers and a copy of the NIT's programming code." The defendant did not specify the reason for any of the requests in the September 9 letter, nor did he define what he meant by the "NIT programming code" or articulate why any of the requested items were material to his defense.

On October 22, 2015, the defendant made a supplemental discovery request seeking information about site visits and images or videos downloaded by persons other than the defendant as well as documents "relating to review and authorization of the FBI's administrative control of the site by the Department of Justice or other

[1] Further detail about the website, investigation, and NIT is contained in the government's response to the defendant's motion to suppress, and attachments thereto. Dkt. 47.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

governmental agencies." Ex. 2. Again, the defendant did not indicate the reason for any of the requests or why they were material to his defense.

On October 30, 2015, the government responded in writing to the defendant's discovery requests and provided detailed information regarding the deployment of the NIT and the information it collected. Ex. 3. With respect to the defendant's request for a detailed description of the computer instructions downloaded by target computers, the government stated exactly what information those instructions directed the defendant's 'activating' computer to transmit – i.e., that "[t]he computer instructions downloaded onto a target's computer (hereinafter 'activating' computer) directed the 'activating' computer to transmit . . . to a computer controlled by or known to the government" the computer's IP address, a unique identifier generated by the NIT to distinguish the data from other computers, information about whether the NIT had already been delivered to the computer, and the computer's operating system, "Host Name," active operating system username, and Media Access Control ("MAC") address. *Id*., pp. 2-3. With respect to the defendant's request for a detailed description of the means by which those instructions are introduced to target computers, the government provided just such an explanation, that is, "[i]n the normal course of operation, websites send content to a visitor's computer. In accordance with the search warrant authorizing the use of the NIT, when an 'activating' computer requested content from Website A, Website A augmented the requested content with the additional computer instructions associated with the NIT." *Id*., p. 3. In response to the defendant's request for a "complete copy of all information and data that was received by the Government in connection with Mr. Michaud's case by means of the NIT, the government provided exactly that information. The information was provided in a comprehensive "user report" that includes information and data about the defendant's actions on the website at issue during the time it was under government control, including the web pages he accessed and the image files present on those pages,

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

as well as all of the information collected by the court-authorized NIT.[2] As noted in the government's response, that information was "contained in the user report that was made available for your review on October 29, 2015, and was also provided to you on a CD on the same date (redacted of digital images that include illegal child pornography)." *Id.*

Although it was not required to do so, the government even provided the defense with further information to assist in its review of that user report, pinpointing for the defense exactly when the NIT was deployed to Michaud's computer and identified his IP address. Specifically, that "On February 28, 2015, after logging on to the website with the previously established username 'Pewter,' Mr. Michaud, using his Windows computer with hostname 'Main' and Windows Username 'Gullible,' navigated to the section of the website entitled 'Pre-teen Videos >> Girls HC'" and that, "[a]fter accessing this section of the website, Mr. Michaud clicked on a specific post entitled, 'Girl 12ish eats other girls/dirty talk,'" which posting "purported to contain links to images and videos of child pornography." *Id*., pp 3-4. The letter advised that the "NIT was deployed to Mr. Michaud's computer after he opened this particular post in the "Pre-teen Videos >> Girls HC" section." *Id*., p. 4. The government also clarified for Mr. Michaud that "only a limited set of information was collected through the court-authorized use of the NIT, which information [was] specified above and in the user report," whereas other information disclosed to him via the user report – including all of the web pages Michaud accessed while FBI had administrative control over the site – "was collected through request data and website logs which were not a function of the NIT." *Id*. The report makes clear that no information, other than that authorized to be collected by the NIT, was collected as a function of the NIT.

With respect to the request for site visits or images and videos posted by persons other than the defendant, even though the government asserted that the actions of other

---

[2] In consideration of 18 U.S.C. § 3509(m), which requires that property that constitutes child pornography remain in the care, custody and control of the government or the court, the government allowed the defense team to inspect and review a copy of that user report which contained child pornography images, and also provided a copy of the report for the defense team to retain, which copy had been redacted of child pornography images.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

users were not material to his defense, the government also provided for review by Mr. Michaud's defense team an offline copy of "Website A." Members of the defense team can sit at a computer and navigate through the pages of the website as a user could when the website was online. That offline copy was initially made available for review on November 4, 2015, and remains available for defense team review and inspection during the pendency of this litigation. Postings and information that were on the website as of the time it ceased operating are accessible via that offline copy and the government's response noted that it would "continue to make [the offline copy] available for [his] inspection and review." *Id*., p. 5.

With respect to the request for documents relating to review and authorization of the FBI's administrative control of the site by the Department of Justice or other governmental agencies, which the government asserted were not material to Michaud's defense, the government responded that Fed. R. Crim. P. 16(a)(2) "does not authorize the discovery or inspection of reports, memoranda, or other internal government documents made by an attorney for the government or other government agent in connection with investigating or prosecuting the case" and further asserted that the requested information was subject to law enforcement privilege "and/or other privileges pertaining to the deliberations of government attorneys or officials." Ex. 1, p. 6. The government accordingly declined to provide information in response to the request. *Id*.

In addition to the materials noted above, the government has provided voluminous discovery materials pertaining to the investigation, well beyond those required pursuant to Fed. R. Crim. P 16. That information includes multiple search warrants, a wiretap application and authorization, and investigative reports, including the forensic reports regarding defendant's digital devices. The government has also made available for the defendant's inspection and review forensic image copies of computers and electronic devices seized from the defendant's residence and person. The defendant concedes that the procedures for the defense team's review of those items are adequate. Dkt. 42, n. 2. Before filing his motion to compel, Michaud did not advise the government of why he

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

believed any of the requested items were material to his defense, nor did he seek other information in lieu of what the government declined to produce that may suffice to facilitate arguments that he has now already made regarding suppression and dismissal of the case.

II. LAW AND ARGUMENT

Under Rule 16, a criminal defendant has a right to inspect documents, data, or tangible items within the government's "possession, custody, or control" that are "material to preparing the defense." Fed. R. Crim. P. 16(a)(1)(E). Evidence is "material" under Rule 16 only if it is helpful to the development of a possible defense. *United States v. Olano*, 62 F.3d 1180, 1203 (9th Cir. 1995). A defendant must make a "threshold showing of materiality" in order to compel discovery pursuant to Rule 16(a)(1)(E). *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir.1995). "Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense." *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990) (emphasis added). "[O]rdering production by the government without any preliminary showing of materiality is inconsistent with Rule 16." *Mandel*, 914 F.2d at 1219. In fact, "[w]ithout a factual showing there is no basis upon which the court may exercise its discretion, and for it to ignore the requirement is to abuse its discretion." *Mandel*, 914 F.2d at 1219. Moreover, Rule 16 "does not authorize a fishing expedition." *United States v. Rigmaiden*, 844 F. Supp. 2d 982, 1002 (D. Ariz. 2012). That is exactly what the defense request amounts to.

A. NIT Programming Code

Michaud seeks a copy of the NIT programming code for three stated reasons: (1) "so that [his] computer forensics expert can independently determine the full extent of the information the Government seized from [his] computer when it deployed the NIT," (2) "whether the NIT interfered with or compromised any data or computer functions," and (3) "whether the Government's representations about how the NIT works in its warrant

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

applications were complete and accurate." Dkt. 54 at 1-2. He contends that the information is relevant to his already-filed motion to suppress and a "potential" motion pursuant to *Franks v. Delaware*. *Id.* He presents no factual information whatsoever in support of the speculative assertions, and fails to show materiality regarding any of those reasons for the requested information. Accordingly, the court should deny his motion. The government addresses the defendant's proffered reasons for requesting the programming code in turn.

1. The extent of information seized from Michaud's computer

As the government has disclosed, the NIT programming code consists of computer instructions that caused a user's activating computer to deliver certain authorized information to a computer controlled by the government. Review of the programming code is unnecessary to determine the extent of information seized from Michaud's computer by operation of the NIT because the information collected by the NIT has already been provided to the defense, and that information answers this question. That information includes Michaud's IP address, a unique identifier generated by the NIT to distinguish the data from other computers, information about whether the NIT had already been delivered to the computer, and the computer's operating system, "Host Name," active operating system username, and Media Access Control ("MAC") address. As the defendant has already been advised, that information is contained in and available on the "user report" disclosed on October 29, 2015. The collection of all of that information was authorized by the NIT warrant.

The defendant fails to provide any factual support regarding what other information he suggests might have been collected through the NIT, let alone other information that was collected. In any event, even if the NIT had collected further information, only that further information could be subject to suppression as outside the scope of the warrant. Because there is no further information, there is no information to suppress, and no compelling need for the defendant's expert to independently determine the information obtained via the NIT.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

The defendant also fails to provide any information to this court to indicate what he considers to be programming code, or to meet his burden of why or how review of the programming code, as opposed to reviewing the information collected by the NIT (or other information the government could provide, other than the programming code), would answer any question about what information the NIT collected. Accordingly, he fails to show how review of the programming code would reveal "the full extent of the information the Government seized from Mr. Michaud's computer" – particularly in light of the fact that the information collected by the NIT has been disclosed to the defendant. The defendant therefore fails to make the required threshold showing of materiality or to present facts that tend to show the government is in possession of information helpful to the defense.

2. Whether the NIT interfered with or compromised any data or computer functions

Review of the programming code is also not material for the purpose of determining whether the NIT interfered with or compromised any data or computer functions. The defendant presents no information to support this wholly speculative hypothesis. Nor does he provide any information regarding what he means by interfering with or compromising any data or computer functions. He also does not explain how, if such interfering with or compromise of data or computer functions did occur – and it did not – this fact would lead to suppression of any evidence, since the only evidence 'seized' was authorized by the warrant. Finally, he has not made any showing of how review of the programming code would provide information to support an argument for some sort of relief if the NIT did interfere with or compromise any data or computer functions, or impact upon any defense regarding child pornography materials found on his computers. This is exactly the type of fishing expedition that Rule 16 does not allow.

Critically, the defendant, through discovery, has ongoing access to a forensic image copy of his computer and digital devices seized, which he may have examined by a computer forensic expert of his choosing. He has also been provided with substantial

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

information pertaining to his dates of access to the pertinent website, and the date and time at which the NIT identified his IP address accessing the site. Despite having that information, he presents nothing to this Court from any examination of that computer or those devices to support his rank speculation that the NIT could have interfered with or compromised any data or computer functions, let alone that it did. Absent some indication, based in fact, as opposed to speculation and conjecture, that the NIT interfered with or compromised any data or computer functions – something the government disputes occurred – the defendant fails to "present facts which would tend to show that the Government is in possession of information helpful to the defense" but rather relies upon "conclusory allegations of materiality" which do not suffice to meet his burden to demonstrate materiality. *Mandel*, 914 F.2d at 1219.

3. Whether the Government's representations about how the NIT works in its warrant applications were complete and accurate

Review of the programming code is also not material for the purpose of determining whether representations about how the NIT works in its warrant applications were complete and accurate. By its nature, this is an entirely speculative request that any defendant could make, at any time, in any case, in an effort to justify any request for information from the government. The defendant presents no facts to suggest that the government is in possession of any information helpful to the defense on that issue. That rank speculation cannot support a finding of materiality of the information. In fact, this sort of speculative request turns the criminal discovery process on its head. If the standard for obtaining criminal discovery were – 'what if the government's representations were not correct or complete' – then there would be no limitation to criminal discovery and every defendant would be entitled to fish through every scrap of information in the government's possession in order to look for something that might impeach a government representation. That is inconsistent with Rule 16, *Brady* and *Giglio*. A defendant can always allege, absent any factual support, that it is arguably possible that the government did not include complete and accurate information in a

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

warrant. A mere allegation simply will not supply a basis for seeking to rummage through the government's files. However, "[w]ithout a factual showing there is no basis upon which the court may exercise its discretion" to require discovery on this point, and if the Court were to ignore that requirement, as the defendant wishes it to do, "is to abuse its discretion." *Mandel*, 914 F.2d at 1219.

The defendant relies upon *United States v. Cedano-Arellano*, 332 F.3d 568 (9th Cir. 2003) (per curiam) to justify his requests for access to the NIT programming code.[3] That case does not support his argument. In that case, the Ninth Circuit found that the District Court's denial of discovery, pursuant to Rule 16, regarding the certification documents and training materials pertaining to a drug dog that had alerted on a defendant's car, whose handler specifically testified about the dog's certification, testing and training at a pre-trial hearing, was an abuse of discretion. *Cedano–Arellano*, 332 F.3d at 571. The court found that the training and certification materials at issue, which were clearly identified and defined by the defendant and whose pertinence was specifically described, were "crucial to [defendant's] ability to assess the dog's reliability" and "to conduct an effective cross-examination of the dog's handler." *Id.* Here, the defendant makes no showing as to how the NIT programming code, as opposed to other information that has been or could be made available, would actually further his defense. Rather, he merely speculates that such a review might produce information could impeach the NIT warrant. Such speculation is not sufficient to trigger a disclosure obligation. *Cf. United*

[3] The defendant's citation to *Gamez-Orduno* is also unavailing. In that case, the government had failed to disclose a written report of a proffer session with a witness that the District Court determined to be material in that statements during the proffer were inconsistent with factual representations and argument made by the government. The District Court, after reviewing the document and determining that it contradicted facts and argument presented by the government, ordered its disclosure and continued a pre-trial hearing. The only issue decided by the Ninth Circuit as to that issue was to affirm the District Court's decision not to dismiss the case, because the pertinent hearing was continued so that the defendants could make use of the information. While the Court recognized the general premise that withholding evidence, where it has been determined that the evidence is material and helpful to the accused, at a motion to suppress may violate due process if "there is a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different," and that "[s]uch a due process violation may be cured . . . by belated disclosure of evidence, so long as the disclosure occurs at a time when disclosure would be of value to the accused," the Ninth Circuit did not require any disclosures to be made. *Id.*, 235 F.3d at 461-62 (internal quotations omitted).

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

States v. Guzman-Padilla, 573 F.3d 865, 890 (9th Cir. 2009) ("[M]ere speculation about materials in the government's files [does not require] the district court ... under *Brady* to make the materials available for [appellant's] inspection.")(citation omitted). Absent the required factual showing, the defendant's request amounts to nothing more than a fishing expedition which is not sanctioned by Rule 16 or any other law.

The defendant also contends that the government's disclosure of information pertaining to a different network investigative technique in another case is relevant to the inquiry in this case. It is not. The *Cottom* case in the District of Nebraska, No. 13-cr-108, involves a different investigation, of a different website, using a different investigative technique than the one pertinent to the defendant's case. That investigative technique was publicly-sourced and no longer in use – in fact, example programming code for the technique was available for review on a public website. After the completion of suppression hearings and before trial, the government disclosed, in an expert notice, information about government expert witnesses, including details about the specific investigative technique used in that case, about which those experts were to testify at trial. The government did not, in that case, as it does here, challenge whether defendants in that case had met their burden to demonstrate materiality related to the disclosed information. Further, there, unlike here, the government did not assert that the particular technique was subject to law enforcement privilege, *see infra*, as that technique was publicly available.

B. Site visits and images/videos accessed by others

Michaud next seeks information about site visits and images or videos downloaded by persons other than him during the brief 14-day period the government operated the website. He claims the information is pertinent to his motion to dismiss regarding alleged "outrageous government conduct," purportedly to show "the extent to which the Government distributed child pornography during the FBI's control and administration of 'Website A.'" Dkt. 54 at 3. This information is immaterial and not discoverable under Rule 16 as it is unrelated to the defendant's guilt or innocence. See

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

United States v. Armstrong, 517 U.S. 456, 462-63 (1996). In any event, information about actions of other users is available for defense review.

The defendant has filed a motion to dismiss the Indictment in this case alleging "outrageous government conduct" in connection with the FBI allowing "Website A," which had already operated for over six months, to continue operating for a brief additional two-week period in February and March of 2015, in order to deploy a court-authorized NIT and conduct court-authorized monitoring of user communications in an attempt to identify users of the site who were sexually exploiting children online. This site had been operating for over six months before the FBI seized it. The information requested is not material to the resolution of that motion, to which the government will separately respond. The crux of the defendant's argument is that it was inappropriate for the FBI to allow such a website to continue operating so that it could attempt to identify its users who were hiding their actual location via the Tor anonymity network. It is undisputed that users, including Michaud, could, and did, visit the website and access child pornography images and videos during the brief two-week period that the website operated at a government facility. Neither the number of visitors nor the number of images or videos accessed by users other than Michaud bear on the defendant's defense.

In any event, the defendant has access to information about site use by other users. The government has provided an offline copy of the website for defense review. The defense team will continue to be allowed to review that copy of the website, in order to gather information about other users. For example, the defendant may browse that site in order to review postings made by users during a time frame that he believes to be pertinent. The defendant baldly claims in his motion, without any supporting information, that "the data relating to the discovery request cannot be gleaned from" review of that offline copy. Dkt. 54 at 3, n. 1. On only one occasion, November 4, 2015, the defendant's counsel and investigator reviewed the offline copy of the website. Absent some factual support for his assertion, the defendant again fails to demonstrate the materiality of his requests.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

C. Internal government memoranda related to approval or supervision of the operation

The defendant next seeks internal government memoranda relating to the approval or supervision of the operation for two stated reasons: first, to show "that the FBI's distribution of child pornography as part of that operation was not a mistake or undertaken by agents acting without FBI or DOJ approval, and was in fact a course of action approved by the Government," and second, to purportedly rebut the government's reliance on the "good faith" doctrine with respect to its reasonable reliance upon the court authorization for the NIT. Dkt. 54 at 3-4. The first line of argument relates to defendant's motion to dismiss for outrageous government misconduct, but as noted, Rule 16 does not support discovery in aid of such motions. *See Armstrong*, 517 U.S. at 462-63. Defendant nonetheless fails to demonstrate materiality as to either reason.

The defendant proffers no facts to support his request for information showing that the investigation was a "mistake or undertaken by agents acting without FBI or DOJ approval." To the contrary, the discovery materials provided, including the NIT search warrant and the Title III application paperwork, clearly indicate the scope and purpose of the operation to identify users who were abusing and exploiting children online while masking their location via the Tor network. The NIT search warrant affidavit, which clearly described the operation of the website at a government facility for a limited time in order to identify users, was sworn to by an FBI Special Agent. Dkt. 47, Ex. 1, p. 23, ¶ 30. The Title III application and affidavit, which also clearly described the scope and purpose of the operation, including the website's operation at a government facility for a limited period of time in order to deploy a court-authorized NIT to identify users, was submitted by two Department of Justice attorneys, based on an affidavit sworn to by an FBI Special Agent, and approved, as all Title III applications are required to be, by a Deputy Assistant Attorney General of the Department of Justice's Criminal Division. Dkt. 47, Ex. 5, App., p. 8 and Ex. A; Aff., p. 31, ¶ 53. To the extent that the defendant wishes to argue that the approval of this operation was somehow an indication of

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

"outrageous government conduct," which frivolous argument the government will address in a separate pleading, he has been provided sufficient discovery to do so.

The defendant's assertion that internal government documents are material to purportedly rebut the government's reliance on the "good faith" doctrine with respect to law enforcement agents' reasonable reliance upon the court authorization for the NIT is misleading, at best. The defendant puts forth this argument by selectively quoting, out of context, small portions of the government's response to his motion referencing the reasonable, good-faith reliance of "agents" or "law enforcement" on the court-authorization for the NIT, in order to baselessly contend that the government is "suggesting that the Court should consider facts related to DOJ's internal review or approval of the 'Website A' warrants when deciding whether the good faith exception should apply." The government argues in its response to the motion to suppress that agents acted in good faith reliance upon the court-authorization obtained to deploy the NIT, which they did. And, to be sure, the Ninth Circuit has held that "an officer's consultation with a government attorney is of significant importance to a finding of good faith." *United States v. Brown*, 951 F.2d 999, 1005 (9th Cir. 1991). But neither pointing out that legal premise nor making that argument implicates documents related to internal deliberations of government attorneys.

In any event, Fed. R. Crim. P. 16(a)(2) "does not authorize the discovery or inspection of reports, memoranda, or other internal government documents made by an attorney for the government or other government agent in connection with investigating or prosecuting the case." Accordingly, the requested materials are specifically excluded from discovery under Rule 16. Furthermore, the sort of documents the defendant seeks – internal government memoranda prepared before the operation was initiated and related to the process by which the investigation proceeded, which would contain the thoughts, impressions opinions, recommendations or advice of government attorneys, and which were prepared in anticipation of litigation – are subject to protection by various privileges, including the deliberative process privilege and attorney work product

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

privilege. *See United States v. Fernandez*, 231 F.3d 1240, 1246-47 (9th Cir. 2000) (applying deliberative process and work product privileges to bar production of death penalty evaluation form and prosecution memorandum). The Court should accordingly deny the defendant's request for those documents.

D. The NIT programming code is subject to a qualified law enforcement privilege

If the Court finds, as it should, that the defendant fails to meet his burden to show that the requested information is material, and otherwise discoverable under Rule 16, that will resolve the defendant's motion. In the event the Court were to determine that the NIT programming code is material to Michaud's defense, however, then the requested information pertaining to the programming code for the NIT is still subject to a qualified law enforcement privilege, as its disclosure would be harmful to the public interest, in that it could diminish the future value of important investigative techniques, allow individuals to devise measures to counteract these techniques in order to evade detection, discourage cooperation from third parties and other governmental agencies who rely on these techniques in critical situations, and possibly lead to other harmful consequences not suitable for inclusion in this response. The United States accordingly requests that the Court hold an *ex parte in camera* hearing, in the event it determines the defendant's request for programming code is material, to consider the United States' claim of privilege and its reasons for non-disclosure.

The Supreme Court, in *United States v. Roviaro*, recognized a qualified "informer's privilege" that protects the identity of government informants. *Roviaro*, 353 U.S. 53, 59 (1957). Courts have since extended the qualified privilege in *Roviaro* to cover other investigative techniques, including traditional and electronic surveillance. *See United States v. Green*, 670 F.2d 1148, 1155 (D.C. Cir. 1981) (upholding the privilege over the defendant's request to learn the location of an observation post used in a drug investigation); *United States v. Van Horn*, 789 F.2d 1492, 1507 (11th Cir. 1986) (recognizing that the privilege applies to the nature and location of electronic surveillance

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

equipment and upholding the privilege over the defendant's request to learn the type and placement of microphones in a co-defendant's office); *In re The City of New York*, 607 F.3d 923, 928-29 (2d Cir. 2010) (upholding privilege regarding reports made by undercover agents). The purpose of the privilege is, among other things, "to prevent disclosure of law enforcement techniques and procedures." *In re Dep't of Investigation*, 856 F.2d 481, 484 (2d Cir. 1988); *Commonwealth of Puerto Rico v. United States*, 490 F.3d 50, 64 (1st Cir. 2007).

The government bears the initial burden of showing that the law enforcement privilege applies to the materials at issue, *In re The City of New York*, 607 F.3d at 944, and the courts then apply a balancing test in determining whether disclosure is required. *Van Horn*, 789 F.2d at 1508. The court will consider the defendant's "need [for] the evidence to conduct his defense and [whether] there are . . . adequate alternative means of getting at the same point. The degree of the handicap [to the defendant] must then be weighed by the trial judge against the policies underlying the privilege." *United States v. Harley*, 682 F.2d 1018, 1020 (D.C. Cir. 1982); *United States v. Cintolo*, 818 F.2d 980, 1002 (1st Cir. 1987). In striking this balance, the Court should also keep in mind that the need for disclosure is more limited in the context of a suppression hearing than at trial. *See McCray v. Illinois*, 386 U.S. 300, 311 (1967); *see also Rigmaiden*, 844 F. Supp. 2d at 990 (applying *McCray* in the context of motion for disclosure of electronic tracking equipment). Even if the party seeking disclosure successfully rebuts the presumption (by a showing of, among other things, a "compelling need"), the court must still then weigh the public interest in non-disclosure against the need of the litigant for access to the privileged information before ultimately deciding whether disclosure is required. *In re The City of New York*, 607 F.3d at 948.

To assess the applicability of the subject privilege and the need for the materials, the court should hold an evidentiary hearing in chambers, a procedure that the Ninth Circuit and other circuits has consistently approved. *See, e.g., United States v. McLaughlin*, 525 F.2d 517, 519 (9th Cir. 1975) (upholding trial court's conduct of *in*

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

camera hearing regarding disclosure of informant's identity and determining that disclosure was not required); *United States v. Alvarez*, 472 F.2d 111, 112-13 (same); *Van Horn*, 789 F.2d at 1508 (district court held *in camera* hearing); *In re Department of Homeland Security*, 459 F.3d 565, 569-71 (5th Cir. 2006) (instructing the district court in a civil case to "review the documents at issue *in camera* to evaluate whether the law enforcement privilege applies"). At an *ex parte in camera* hearing, the United States will be available to present more detailed information about the NIT programing code and its concerns about disclosure. Because of the sensitivity of the technique and for other reasons the United States can present at an *ex parte in camera* hearing, disclosing the programming code pursuant to a protective order is inadequate.

Upon a finding that the privilege applies, Defendant must show that his need for the information overcomes the public interest in keeping it secret. *See Van Horn, 789 F.2d at 1507*. The public interest in nondisclosure here significantly outweighs defendant's need for the information, particularly in light of the defendant's speculative claims regarding the materiality of the programming code. In particular, the risk of circumvention of an investigative technique if information is released has been recognized as a factor in applying law enforcement privilege to electronic surveillance. *See Van Horn*, 789 F.2d at 1508.[4] Accordingly, in the event the Court finds the requested information to be material, the Court should hold an *ex parte, in camera* hearing to assess the applicability of the privilege and the defendant's need for the materials.

[4] Risk of circumvention has also been accepted by numerous courts as a basis for non-disclosure, in the civil FOIA context. *See, e.g., James v. U.S. Customs and Border Protection*, 549 F.Supp.2d 1, 10 (D.D.C. 2008) (concluding that CBP properly withheld information under FOIA that "could enable [others] to employ measures to neutralize those techniques"); *Judicial Watch v. U.S. Department of Commerce*, 337 F.Supp.2d 146, 181-82 (D.D.C. 2004) ("even commonly known procedures may be protected from disclosure if the disclosure could reduce or nullify their effectiveness").

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

III. CONCLUSION

For all the foregoing reasons, the Court should deny Defendant's motion to compel.

Dated this 4th day of December, 2015.

Respectfully submitted,
ANNETTE L. HAYES
United States Attorney

s/ S. Kate Vaughan
S. KATE VAUGHAN
Assistant United States Attorney
700 Stewart Street, Suite 5200
Seattle, WA
Phone: (206) 553 7970
Fax: (206) 553 0882
E-mail: kate.vaughan@usdoj.gov

STEVEN A. GROCKI
Chief

s/ Keith A. Becker
Trial Attorney
Child Exploitation and Obscenity Section
1400 New York Ave., NW, Sixth Floor
Washington, DC 20530
Phone: (202) 305-4104
Fax: (202) 514-1793
E-mail: keith.becker@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on December 4, 2015, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system. I will provide the motion to the attorney of record for the defendant via Email.

s/ S. Kate Vaughan

S. KATE VAUGHAN
Assistant United States Attorney
700 Stewart Street, Suite 5200
Seattle, WA
Phone: (206) 553 7970
Fax: (206) 553 0882
E-mail: kate.vaughan@usdoj.gov